VALKYRIE COMODO

Summary

File Name: 69c72aaa506368b23c93b30347c56a00f135645deeab5046c695579586eb7fcb.ex

File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed

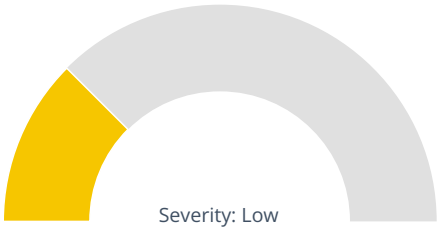
SHA1: 0537f9741eaeb183d6e0e96719fb8f86912615f7

MD5: cd2543a1e63bc31315f59893f4607abf

PUA

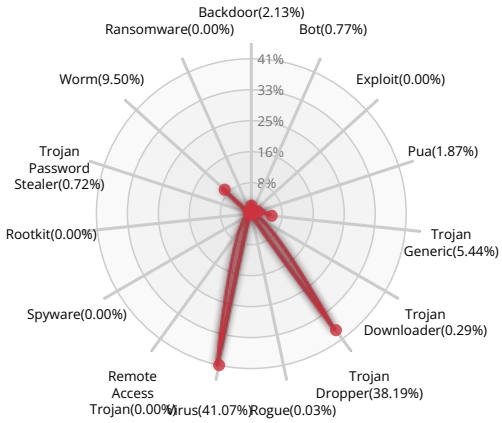
Valkyrie Final Verdict

DETECTION SECTION

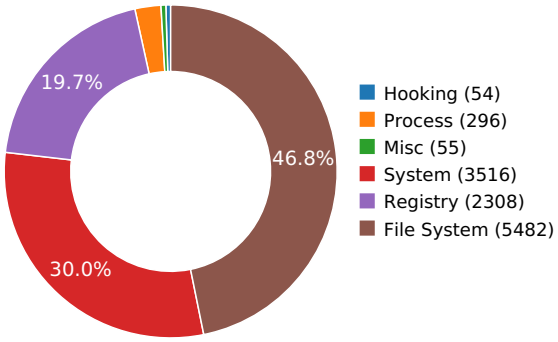


Verdict: PUA

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

PACKER

The executable is compressed using UPX — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Likely virus infection of existing system binary — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time — Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files (x86)
C:\Users\user\AppData\Local\Temp\wininet.dll
C:\Windows\System32\wininet.dll
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local
C:\Users\user\AppData
C:\Users\user
C:\Users
C:\
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202.exe
C:\u
C:\us
C:\use
C:\user
C:\Users\
C:\Users\u
C:\Users\us
C:\Users\use
C:\Users\user\
C:\Users\user\a
C:\Users\user\ap
C:\Users\user\app
C:\Users\user\appd
C:\Users\user\appda
C:\Users\user\appdat
C:\Users\user\AppData\
C:\Users\user\AppData\l
C:\Users\user\AppData\lo
C:\Users\user\AppData\loc

C:\Users\user\AppData\loca
C:\Users\user\AppData\Local\
C:\Users\user\AppData\Local\t
C:\Users\user\AppData\Local\te
C:\Users\user\AppData\Local\tem
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp\0
C:\Users\user\AppData\Local\Temp\05
C:\Users\user\AppData\Local\Temp\053
C:\Users\user\AppData\Local\Temp\0537
C:\Users\user\AppData\Local\Temp\0537f
C:\Users\user\AppData\Local\Temp\0537f9
C:\Users\user\AppData\Local\Temp\0537f97
C:\Users\user\AppData\Local\Temp\0537f974
C:\Users\user\AppData\Local\Temp\0537f9741
C:\Users\user\AppData\Local\Temp\0537f9741e
C:\Users\user\AppData\Local\Temp\0537f9741ea
C:\Users\user\AppData\Local\Temp\0537f9741eae
C:\Users\user\AppData\Local\Temp\0537f9741eaeb
C:\Users\user\AppData\Local\Temp\0537f9741eaeb1
C:\Users\user\AppData\Local\Temp\0537f9741eaeb18
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e9
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e967
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e9671
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719f
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8

C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f8
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f869
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f8691
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f869126
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f8691261
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Trickler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Qwertyuio\Trickler\Deleting

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202a.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202b.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202c.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202d.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202e.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202f.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202g.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202h.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202i.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202j.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202k.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202l.exe

C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202m.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202n.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202o.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202p.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202q.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202r.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202s.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202t.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202u.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202v.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202w.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202x.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202y.exe

RESOLVED APIS

kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
advapi32.dll.SetNamedSecurityInfoA
advapi32.dll.GetNamedSecurityInfoA
ntmarta.dll.GetMartaExtensionInterface
wininet.dll.InternetGetConnectedState
wininet.dll.InternetErrorDlg
wininet.dll.InternetAttemptConnect
wininet.dll.InternetQueryOptionA
wininet.dll.InternetOpenA
wininet.dll.InternetConnectA
wininet.dll.InternetCloseHandle
wininet.dll.InternetReadFile
wininet.dll.InternetOpenUrlA
wininet.dll.InternetSetStatusCallback
wininet.dll.InternetSetOptionA
wininet.dll.InternetGetLastResponseInfoA
wininet.dll.HttpOpenRequestA
wininet.dll.HttpSendRequestA
wininet.dll.HttpQueryInfoA

wininet.dll.InternetCanonicalizeUrlA
wininet.dll.InternetCombineUrlA
wininet.dll.InternetCrackUrlA
wininet.dll.HttpAddRequestHeadersA

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\Software
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\software\QwertTest
HKEY_LOCAL_MACHINE\software\QwertTest\Qwertyui
HKEY_LOCAL_MACHINE\software\Qwertyuio\Trickler
HKEY_LOCAL_MACHINE\Software\CLASSES\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}\uets
HKEY_LOCAL_MACHINE\software\Qwertyuio
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}\
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Trickler
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Qwertyuio\Trickler\AppPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Qwertyuio\Trickler\OldTrickler
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Qwertyuio\Trickler\Deleting
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Qwertyuio\Trickler
HKEY_LOCAL_MACHINE\software\Qwertyuio\Qwert\stat\GMT\Settings
HKEY_LOCAL_MACHINE\software\Qwertyuio\CMEII

HKEY_LOCAL_MACHINE\software\Qwertyuio\Date Manager

EXECUTED COMMANDS

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202a.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202b.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202c.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202d.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202e.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202f.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202g.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202h.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202i.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202j.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202k.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202l.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202m.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202n.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202o.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202p.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202q.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202r.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202s.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202t.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202u.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202v.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202w.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202x.exe

c:\users\user\appdata\local\temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202y.exe

READ FILES

C:\Windows\System32\tzres.dll

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7.exe

C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202.exe

C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202a.exe

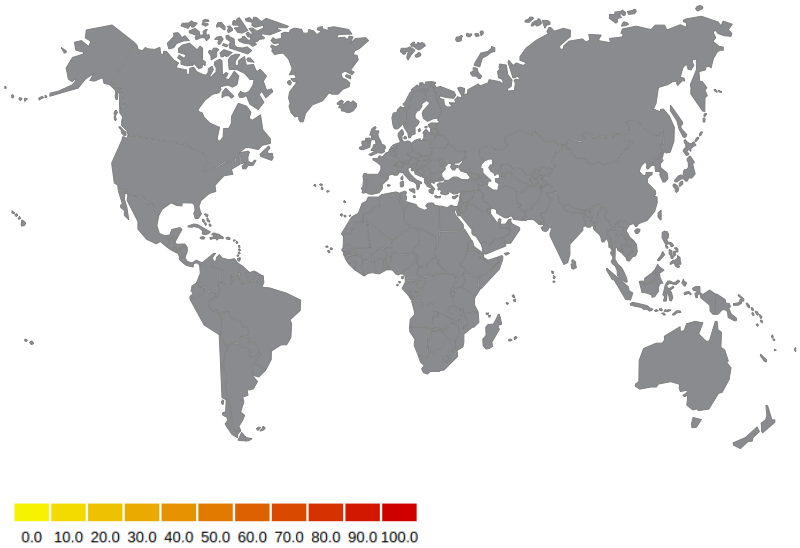
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202b.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202c.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202d.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202e.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202f.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202g.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202h.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202i.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202j.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202k.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202l.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202m.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202n.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202o.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202p.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202q.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202r.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202s.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202t.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202u.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202v.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202w.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202x.exe
C:\Users\user\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202y.exe

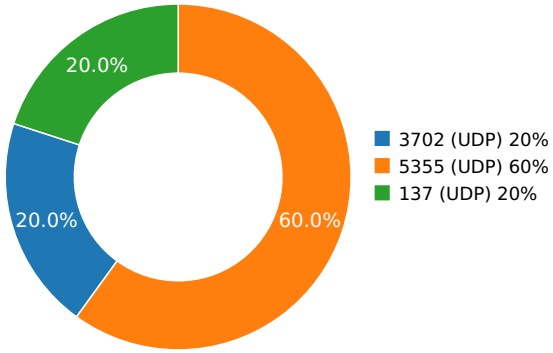
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\CLASSES\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}\uets
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Trickler
HKEY_LOCAL_MACHINE\software\Qwertyuio\Trickler
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Qwertyuio\Trickler\AppPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Qwertyuio\Trickler\OldTrickler

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.88969492912	Sandbox	224.0.0.252	5355
6.89670395851	Sandbox	224.0.0.252	5355
6.90310406685	Sandbox	239.255.255.250	3702
6.93894791603	Sandbox	192.168.56.255	137
9.51935791969	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202f.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 658f7c8255cfab9fd088b2adeee25ca9 **SHA-1 :** b81cf3718e8faf01844d58771010bb201f2d2621 **SHA-256 :** bed35f184bda13bb08275261ecb5fecfc6cb88dd **SHA-512 :** 0dbe33d57476d4af2282370eeb789a2b34949a7 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202l.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 626452015e41113db5faf3518151b640 **SHA-1 :** ca7d6dcf22eb1cccaf9f99d52000b1d050e79639 **SHA-256 :** cbd503c77af6f71c61a58c71c7ca8fa5b3163478a **SHA-512 :** eb172ec37daca13f0a3484d38035059cb335062a **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202r.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** ce78747df085f674ac29868fc2189cab **SHA-1 :** b1faf9c520341ba83170105d4912a721c5ede737 **SHA-256 :** 92ae089a0cb9c83d39e9a23bdda2832225df12a7 **SHA-512 :** d17acc226da72e121a8cebae857c091ac139a16f **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202o.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 7df3310beaf605ce9f9247ff3a5ddc63 **SHA-1 :** 454d9d2a47f8ff22a3a78e2b94719f884711a913 **SHA-256 :** 4acec04d76ef685cc0abcd010e454777fea24d757 **SHA-512 :** 94ab9a0d3da813d5497ce364b34a812a339e2ce **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 55baeba3081884e3b93216c6b63841c5 **SHA-1 :** 7a787036dce4588ff415824c23b79e4fe8d1cb65 **SHA-256 :** 30d55419d3b77fd6747fa0ea2d7e9fa2e56113b3 **SHA-512 :** 9c2116c39cca8ddf9bc97bfc9bdd59806e7c11e2(**Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202v.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** fc60fdccf9cc77c0f30697de7f2dc553 **SHA-1 :** 88862d15a46d9c360751c626681c2d7860b8fbfa **SHA-256 :** 10a18ad3d6fac96b664698b081214cea9b3b367f **SHA-512 :** 9cb5032cfb58051aaf0847000ee84b799ac620bd **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202n.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 462aa31560634f5b0d60afab1d3c2685 **SHA-1 :** efcdb99625e380535907add13f5da8e053302952 **SHA-256 :** 9b91fc7db7981f0579a58d726604aa4198e45961 **SHA-512 :** 2739b79ab483ed0c2bcc227753bed15892c6185 **Size :** 273.156 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202s.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 59ef0fcc1e13deff49c3945dc8fec01b **SHA-1 :** 335ed1f0ac6a6a5ab810738623a8f9ea4c433dcc **SHA-256 :** 025bf86554ee81a73650a4ca56dd09fbfd739873 **SHA-512 :** 803600a3a40f8447a0dbae885f7d85fad272b3ec **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202c.Exe **C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202d.Exe**	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 329a5b2b6cc2965c9501d2c3dc739c44 **SHA-1 :** c3c32335f6dbd408c559680dc9cef7702c44d5f3 **SHA-256 :** 7f73f11c106bb3696710da6af971e66337e290b0 **SHA-512 :** d9ce6e30961ab2c8496c4cf5086461bb935363f9 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202t.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 8dbf99621f08d2a21d43a17fdabfe617 **SHA-1 :** 645f5c170c05d0c206f0959ea29f0fe16550ed6f **SHA-256 :** 3e0da97d50f123b1d3f82ef42671fcf6f4a36a648 **SHA-512 :** 0e49b19d38ed834abcdcc72afa5a2f737431f2911 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202x.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** c4d43aeaa46fab21da06c2a217cbe33f **SHA-1 :** 37bea8317a0d03121096e0f00932dc621b425a73 **SHA-256 :** 0537263834f3b9a8b58c9fc249082a3c783df9a27 **SHA-512 :** b5595692a9600a106b8ec5b429a8d131d595cbd **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202u.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 7041027172521332e1008da38ecd601f **SHA-1 :** 87995e64a4e66e8f964f4a15f86b498cdd9a65d5 **SHA-256 :** 46c95a2d1f0872ecb3ec6f21263224afe761c040f **SHA-512 :** da88be463ed568734aa676b1fb649c6f0a310d5c **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202i.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** f6b69b7592f3d6dba70701814a6d258f **SHA-1 :** 30a886dbbe547a8f6d657bac096c766229eeab94 **SHA-256 :** dd586b369899e01ef6c69d42c23d53c825ef075f **SHA-512 :** 8531d941ade37fa7167aae953f9f36e85f5823017 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202q.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 2cc5e8c7efd6d791d20eef32d0277cb7 **SHA-1 :** 1feed78f384fa498b77f99d8cfc16dafd2d1bf6b **SHA-256 :** 60198e4ab75d4b1c7a033813e77d053907c2d48 **SHA-512 :** e4297a36dc05fde2b7fc8e96bf44ea13dd226c79 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202g.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** f32fb7cf8309c786bf0aceec27eb4ad1 **SHA-1 :** 55029e02546076c851331ba9f3416f8f5e004269 **SHA-256 :** 691609956779e83b0d69181bcb2ccb7effb968f7 **SHA-512 :** 260c49fbf191ad06985efc190e8d6dd4d5ab17b3 **Size :** 273.156 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202y.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 6c4dfc8246428fbde6e775e281dc032e **SHA-1 :** 3aa98ff2d89169a1cb68516391cd17ec6c37c575 **SHA-256 :** b34555b05497d285eb3659639590077ecdc0376 **SHA-512 :** 604a67629202a97822512c498fe159f45dd9a3d6 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202k.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 6f1278c08fac5abc7e5c62be722741e5 **SHA-1 :** 755021d09398d4de1e49eac9ad6879d68019050c **SHA-256 :** b96e6eb1efbf87b5032b1df42cb7a4b66dfaeaac5 **SHA-512 :** 34b966d679d9ef2ebad29d2ff1eca6295df6d06a **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202h.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** a0fb978d257e16d38552424518d4e5d6 **SHA-1 :** 9e6781603b9a0c1fd2c11767051d6c2888a4e3d1 **SHA-256 :** de78f246ecf73b24a82e454f40c4b42376190060a **SHA-512 :** 2ed4a0a0a768932121981bc43d1295b066b753a **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202b.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 3d2c6d9d57a6ed402c5d1d046fd19e7a **SHA-1 :** 2efcd1509975c7341776c025bf073a53b171c6de **SHA-256 :** 2916503709c3d84f47ef9046a38b99395ce62e8c **SHA-512 :** 6af70067b45cd7c018c6f93ba6f63f0cfd5b36017e **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202a.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** ca97b2ee463d44cac70f7dc3f1dca8c3 **SHA-1 :** f4d68ff4d121db1c92504a4f579014c0b324b8e4 **SHA-256 :** 27cfee4a7d11b60355333d3429cc3eadaef220d0 **SHA-512 :** 066e594424ad3887dacc011b58e8de012430c6d **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202w.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 4874c9224fc4453a904879da7ed10a48 **SHA-1 :** ac2a824048e6ae60d2764d0b5f4234aaa4cad94f **SHA-256 :** 42b3a12f3dfafef6369f17f8a0ee0d833f9afa03eca **SHA-512 :** 98c1b743d5186d9294728c3bc175b6ea8fef6d19 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202e.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 68ceeb8f918738bc7d8ecfb93899cbdb **SHA-1 :** 1c3038f828b326252e7be61ea1696e9dfe7ad410 **SHA-256 :** b8da4a8f0138838c7c0d8e9e6b005de86577bde3 **SHA-512 :** 6063b953fa95a3f82c768b7351498625e44c9e78 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202p.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** af48115ad4ceefc28d49de0e414da9f9 **SHA-1 :** 16599e030e1f03429d0f7114044e5acf93fc45ae **SHA-256 :** 83a45b6fde74229de3d8ab71c8073092c3c45c9c **SHA-512 :** 7373c054afc2e8c9600d6c7c421a76bd0951df51a **Size :** 273.156 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202m.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 260e3985e5e20426728a318174eab44a **SHA-1 :** 03865e1a5cb69f737519ae8753af2c3dcc402a14 **SHA-256 :** d513cf45162d5d07451dda7cad8a8f137d833dc7 **SHA-512 :** b0e1a277d432d13705662b73b4cd524624f4fda4 **Size :** 273.156 Kilobytes.
C:\Users\User\AppData\Local\Temp\0537f9741eaeb183d6e0e96719fb8f86912615f7_3202j.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 3e0481d69c1875671ed4518e580b5b43 **SHA-1 :** 6de753b07b4896c8b714d8acd86a322470f6af57 **SHA-256 :** 869b095d12a96b1e330ef7c47d65369704e7fc4a **SHA-512 :** 2fc9a9c2a447d6c531296a9767461278b2cded5a **Size :** 273.156 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	69c72aaa506368b23c93b30347c56a00f135645deeab5046c695579586eb7fcb.ex
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1:	0537f9741eaeb183d6e0e96719fb8f86912615f7
MD5:	cd2543a1e63bc31315f59893f4607abf
First Seen Date:	2023-07-07 11:50:41.336260 (3 years ago)
Number Of Clients Seen:	5
Last Analysis Date:	2023-07-07 11:50:41.336260 (3 years ago)
Human Expert Analysis Date:	2023-07-07 23:16:40.521102 (3 years ago)
Human Expert Analysis Result:	PUA

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[[27.1, u'Win32 Executable MS Visual C++ (generic)'], [23.5, u'UPX compressed Win32 Executable'], [23.0, u"Win32 EXE Yoda's Crypter"], [11.3, u'Windows screen saver'], [5.7, u'Win32 Dynamic Link Library (generic)']]
Compilation Time Stamp	0x3CC4C509 [Tue Apr 23 02:20:57 2002 UTC]
ProductVersion	5.1.0.0
FileVersion	5.1.0.0
OriginalFilename	divxenc.exe
FileDescription	
Translation	0x0409 0x04e4
Entry Point	0x41be59 (UPX0)
Machine Type	Intel 386 or later - 32Bit
File Size	273156
Ssdeep	6144:jh8Z5hMWNFM8LAurlEzAX7oAwfSZ4sX9zQI:VEXM5qrllX7Xw2EI
Sha256	69c72aaa506368b23c93b30347c56a00f135645deeab5046c695579586eb7fcb
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/0/5/3/7/0537f9741eaeb183d6e0e96719fb8f86912615f7', u'EXE:OriginalFileName': u'divxenc.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:07 11:50:15+00:00', u'EXE:InitializedDataSize': 4096, u'File:FileModifyDate': u'2023:07:07 11:49:01+00:00', u'EXE:FileVersionNumber': u'5.1.0.0', u'EXE:FileVersion': u' 5.1.0.0', u'File:FileSize': u'267 kB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'5.1.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 139264, u'File:FileName': u'0537f9741eaeb183d6e0e96719fb8f86912615f7', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2002:04:23 02:20:57+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/0/5/3/7', u'EXE:FileDescription': u'', u'EXE:EntryPoint': u'0x1be59', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 20480, u'File:FileInodeChangeDate': u'2023:07:07 11:49:01+00:00', u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'5.1.0.0'}]
Mime Type	application/x-dosexec
Imphash	08bca23b44274b89c6980b3fd0bc0ab9

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x22000	0x22000	6.4613655026	6e585c2a2ea059302e83376c71db43a3
UPX1	0x23000	0x16000	0x15a00	4.00855873885	c3ec8c2070c3ac813709cef23f5b1796
.rsrc	0x39000	0x1000	0x600	2.76130880003	ee69ceaa897f3c8ede10c6ddf5c6dc8c
.htext	0x3a000	0x5000	0x5000	3.52040728913	a6c697b6c8f888a1ab486401a44a789a

PE Imports

- KERNEL32.DLL
  - GetTempPathA
  - GetModuleFileNameA
  - FindNextFileA
  - InitializeCriticalSection
  - DeleteCriticalSection
  - EnterCriticalSection
  - LeaveCriticalSection
  - FindFirstFileA
  - ExpandEnvironmentStringsA
  - RemoveDirectoryA
  - GetFileAttributesA
  - DeleteFileA
  - CreateDirectoryA
  - GetFileSize
  - SetFileAttributesA
  - GetShortPathNameA
  - ReadFile
  - GlobalMemoryStatus
  - CreateProcessA
  - GetVersionExA
  - SetEvent
  - OpenEventA
  - WaitForSingleObject
  - MoveFileExA
  - GetDiskFreeSpaceA
  - GetProcAddress
  - LoadLibraryA
  - FreeLibrary
  - LocalFree
  - GetCurrentThread
  - CreateMutexA
  - OpenMutexA
  - InterlockedIncrement
  - InterlockedDecrement
  - GlobalFree
  - GlobalAlloc
  - GetModuleHandleA
  - OutputDebugStringA
  - GetLocalTime
  - CreateEventA
  - GetTempFileNameA
  - FindClose
  - GlobalUnlock
  - GlobalLock
  - ResetEvent
  - CreateThread
  - lstrcmpiA
  - SetEnvironmentVariableA
  - CompareStringW
  - CompareStringA
  - ReleaseSemaphore
  - IsBadCodePtr
  - IsBadReadPtr
  - SetUnhandledExceptionFilter
  - GetStringTypeW
  - GetStringTypeA
  - IsBadWritePtr
  - VirtualAlloc
  - SetEndOfFile
  - SetStdHandle

    - FlushFileBuffers
    - GetOEMCP
    - GetACP
    - GetCPInfo
    - VirtualFree
    - HeapCreate
    - HeapDestroy
    - GetStdHandle
    - SetHandleCount
    - GetEnvironmentStringsW
    - GetEnvironmentStrings
    - FreeEnvironmentStringsW
    - FreeEnvironmentStringsA
    - UnhandledExceptionFilter
    - LCMapStringW
    - LCMapStringA
    - MultiByteToWideChar
    - GetPrivateProfileStringA
    - CopyFileA
    - WriteFile
    - CreateFileA
    - SetFilePointer
    - GetTickCount
    - CloseHandle
    - WritePrivateProfileStringA
    - GetExitCodeProcess
    - GetLastError
    - SetLastError
    - Sleep
    - lstrcatA
    - GetWindowsDirectoryA
    - GetVolumeInformationA
    - lstrlenA
    - lstrcpynA
    - lstrcpyA
    - SearchPathA
    - FormatMessageA
    - GetSystemDirectoryA
    - HeapAlloc
    - GetCurrentThreadId
    - UnmapViewOfFile
    - MapViewOfFile
    - WideCharToMultiByte
    - HeapSize
    - HeapReAlloc
    - GetCurrentProcess
    - TerminateProcess
    - TlsGetValue
    - TlsAlloc
    - TlsSetValue
    - OpenSemaphoreA
    - CreateFileMappingA
    - HeapFree
    - GetFileType
    - ExitProcess
    - GetVersion
    - GetCommandLineA
    - GetStartupInfoA
    - GetSystemTime
    - GetTimeZoneInformation
    - RtlUnwind
- ADVAPI32.dll
    - RegQueryValueExA
    - RegOpenKeyExA
    - RevertToSelf
    - ImpersonateSelf
    - AreAllAccessesGranted
    - GetAclInformation
    - GetAce
    - AllocateAndInitializeSid
    - GetLengthSid
    - InitializeAcl
    - FreeSid
    - InitializeSecurityDescriptor
    - SetSecurityDescriptorDacl

    - RegEnumKeyExA
    - RegQueryInfoKeyA
    - RegEnumValueA
    - RegEnumKeyA
    - RegDeleteKeyA
    - RegDeleteValueA
    - RegCreateKeyExA
    - RegSetValueExA
    - AccessCheck
    - OpenThreadToken
    - RegCloseKey
    - AddAccessAllowedAce
- LZ32.dll
    - LZOpenFileA
    - LZClose
    - LZSeek
    - LZRead
- ole32.dll
    - CoCreateGuid
- USER32.dll
    - GetClassInfoExA
    - WaitForInputIdle
    - DestroyWindow
    - wsprintfA
    - DispatchMessageA
    - TranslateMessage
    - GetMessageA
    - UpdateWindow
    - SetWindowPos
    - ShowWindow
    - IsWindow
    - CreateWindowExA
    - SetRect
    - GetSystemMetrics
    - SystemParametersInfoA
    - RegisterClassExA
    - LoadCursorA
    - LoadIconA
    - DefWindowProcA
    - SetPropA
    - GetPropA
    - KillTimer
    - SetTimer
    - PostMessageA
    - EnumWindows
    - GetClassNameA
    - GetDesktopWindow
    - MessageBoxA
    - PostQuitMessage
    - SetForegroundWindow
    - PeekMessageA
    - GetCursorPos
    - GetWindowTextA
    - FindWindowA
    - IsWindowVisible
- VERSION.dll
    - GetFileVersionInfoSizeA
    - VerQueryValueA
    - GetFileVersionInfoA
- WSOCK32.dll
    - recv
    - WSACleanup
    - WSAStartup
    - WSACancelAsyncRequest
    - inet_addr
    - WSAAsyncGetHostByName
    - getsockopt
    - __WSAFDIsSet
    - select
    - connect
    - htons
    - ioctlsocket
    - bind
    - inet_ntoa
    - socket

- closesocket
- send
- WSAGetLastError

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 233564, u'sha256': u'28a6e2db31f076c3e585edc7ec17119889c16f258abbb674d8a99e8fad9d9234', u'type': u'data', u'size': 432}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS